1. Amendments to the Claims:

1. (Original) A mobile application security system, comprising:

a central computer for controlling the security of a mobile application;

one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution;

the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer;

wherein the security monitoring means further comprises means detecting code of the mobile application marked as immutable and means for replacing the immutable code with code known to be safe by the central computer.

2. (Original) A mobile application security system, comprising:

a central computer for controlling the security of a mobile application;

one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution;

a1 the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer; and

wherein the security monitoring means further comprises means for detecting state data marked as immutable and means for replacing the immutable state data with state data known to be safe by the central computer.

3. (Original) A mobile application security system, comprising:

a central computer for controlling the security of a mobile application;

one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution;

the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer; and

wherein the security monitoring means further comprises means for detecting an itinerary of the mobile application that is marked as immutable and means for replacing the immutable itinerary with an itinerary known to be safe by the central computer.

4. (Original) The system of Claim 3, wherein the itinerary comprises past historical itinerary data.

5. (Original) A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring the security of the mobile application as it jumps between the host computers, wherein the security monitoring further comprises detecting code of the mobile application that is marked as immutable and replacing the immutable code with code known to be safe by the central computer.

6. (Original) A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring the security of the mobile application as it jumps between the host computers,

wherein the security monitoring further comprises detecting a state of the mobile application that is marked as immutable and replacing the immutable state with state data that is known to be safe by the central computer.

7. (Original) A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring the security of the mobile application as it jumps between the host computers, wherein the security monitoring further comprises detecting an itinerary of the mobile application that is marked as immutable and replacing the immutable itinerary with itinerary data known to be safe by the central computer.

8. (Original) The method of Claim 7, wherein the itinerary comprises past historical itinerary data.

9. (New) The system of Claim 1, wherein the security monitoring means further comprises means for inspecting the access control list of the mobile application to determine if the code of the mobile application is marked as immutable.

10. (New) The system of Claim 2, wherein the security monitoring means further comprises means for inspecting the access control list of the mobile application to determine if the state data of the mobile application is marked as immutable.

11. (New) The system of Claim 3, wherein the security monitoring means further comprises means for inspecting the access control list of the mobile application to determine if the itinerary of the mobile application is marked as immutable.

12. (New) The method of Claim 5, wherein the security monitoring further comprises inspecting the access control list of the mobile application to determine if the code of the mobile application is marked as immutable.

13. (New) The method of Claim 6, wherein the security monitoring further comprises inspecting the access control list of the mobile application to determine if the state data of the mobile application is marked as immutable.

14. (New) The method of Claim 7, wherein the security monitoring further comprises inspecting the access control list of the mobile application to determine if the itinerary of the mobile application is marked as immutable.

15. (New) A mobile application security method, comprising:

receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host; and

monitoring the security of the mobile application as it jumps between the host computers, wherein the security monitoring further comprises:

saving the mobile application code when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is trusted,

stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted,

replacing the code of the mobile application when the code is marked as immutable and the mobile application has been dispatched in the past, and

saving the code of the mobile application when the code is not marked as immutable.

16.(New) A mobile application security system, comprising:

a central computer for controlling the security of a mobile application;

one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution;

the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer;

wherein the security monitoring means further comprises:

means for saving the mobile application code when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is trusted,

means for stripping the code from the mobile application when the code is marked as immutable, the mobile application has not been dispatched in the past and the host dispatching the mobile application is not trusted,

means for replacing the code of the mobile application when the code is marked as immutable and the mobile application has been dispatched in the past, and

means for saving the code of the mobile application when the code is not marked as immutable.